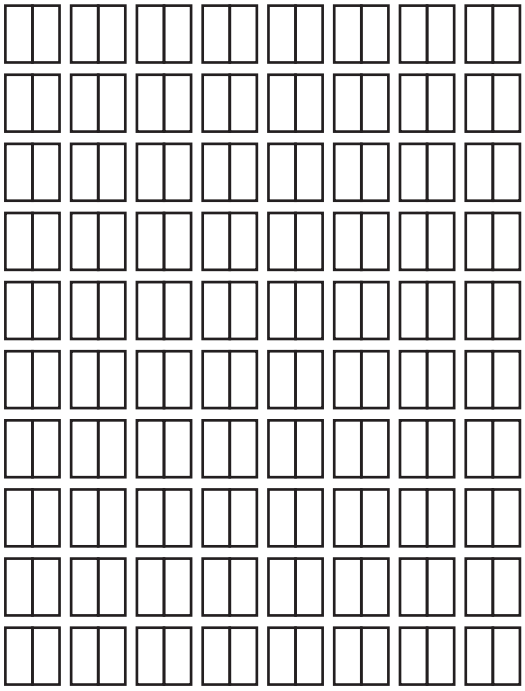
Strong Encryption with a 10-Sided Die

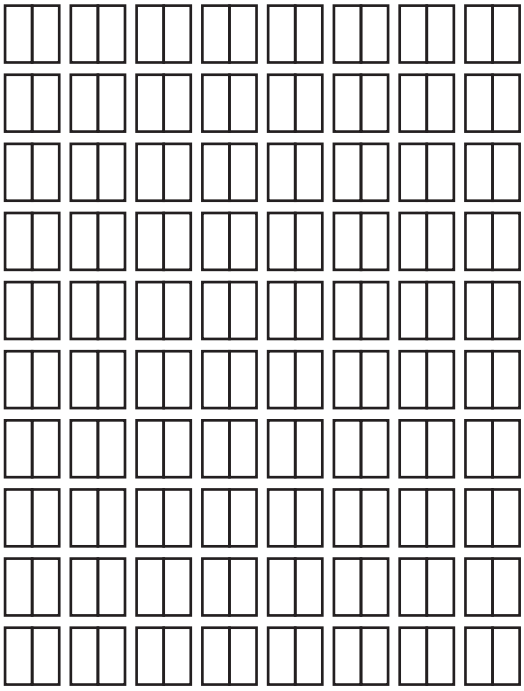
a how-to guide from

IFFY BOOKS
319 N. 11th St. #3D
Philadelphia, PA 19107

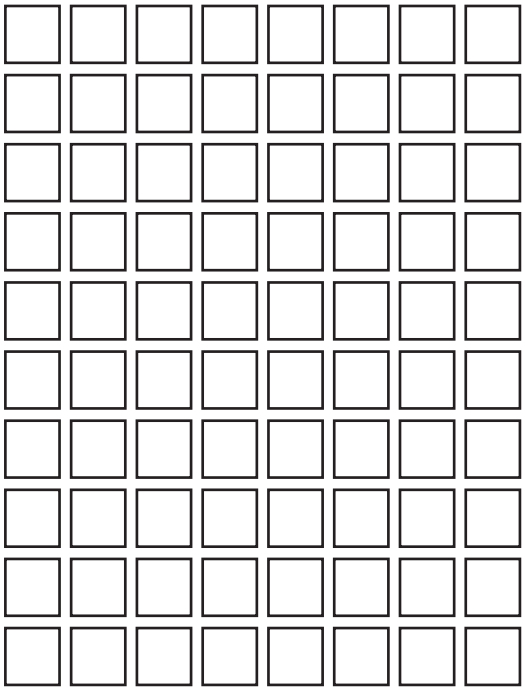
Your private key (burn after encoding)



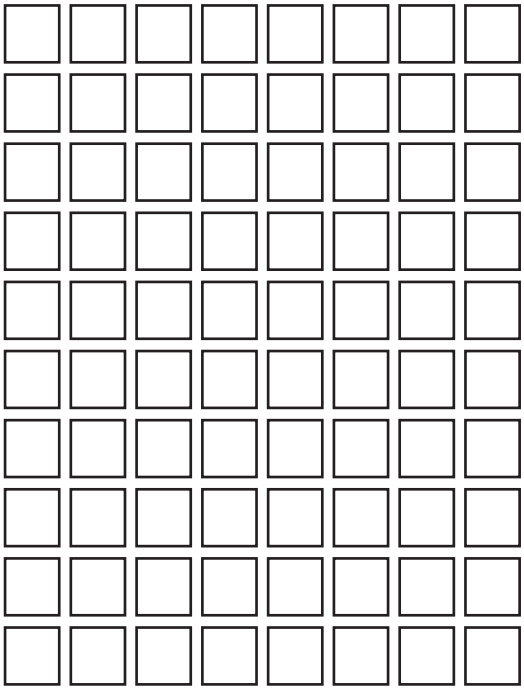
A private key for your friend



Plaintext (burn after encoding)



Ciphertext



How do you send a private message if you don't trust your computer? Use a 10-sided die to make a one-time pad.

Have you ever wanted to send a secret message to a friend? If so, you've probably wondered whether the channel you're using is really secure. Even if an encrypted chat program works as advertised, it's all for naught if someone is logging your keystrokes.

If you're looking for mathematically guaranteed secrecy, consider using a **one-time pad cipher**. As long as you and your friend follow some simple rules, you'll be able to send messages that can't be cracked by any computer program.

This zine will teach you to send and receive messages using a one-time pad cipher. First you'll use a 10-sided die to generate your **private key**. Then you'll use your key to encrypt a short message, which your friend can decode with their copy of the key.

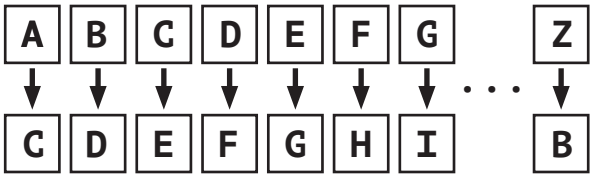
You might expect strong encryption would require using a computer, but all you need to make a one-time pad cipher is a piece of paper, a pencil, and a source of random numbers.

The biggest downside of using a one-time pad cipher is that you'll need to share a private key with the friend you're corresponding with before sending an encrypted message. Since each key can only be used once, you may want to generate a number of keys ahead of time.

What is a cipher?

A **cipher** is any technique for converting a **plaintext** message into an encrypted form called a **ciphertext**. The goal is to generate a ciphertext that is unreadable to anyone except the intended recipient.

You may be familiar with **rotation ciphers**, also known as Caesar ciphers. For example, in a so-called ROT-2 cipher, each letter in the plaintext is replaced with the letter two spaces ahead in the alphabet.



Rotation ciphers are OK for passing notes in class, but they're easy to decode even if you don't know the rotation value. That's because people use certain letters, such as **e**, **t**, and **a** in English, more frequently than others. If you send a message using a rotation cipher, an adversary can count how many times each letter appears in the ciphertext, then make some guesses and reconstruct the plaintext.

Or an adversary can use a brute force approach, testing every possible rotation value to see which one outputs a message that looks like English.

!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú

space →

Cursor strip

Encoder/Decoder Lookup Table

encoder	decoder	
00	00	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú
01	99	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú
02	98	“#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !
03	97	#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"
04	96	$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#
05	95	%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$
06	94	&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%
07	93	'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&
08	92	()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'
09	91	)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'(
10	90	*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()
11	89	+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*
12	88	,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+
13	87	-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,
14	86	./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-
15	85	/0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-.
16	84	0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./
17	83	123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0
18	82	23456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./01
19	81	3456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./012
20	80	456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123
21	79	56789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./01234
22	78	6789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./012345
23	77	789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456
24	76	89:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./01234567
25	75	9:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./012345678
26	74	:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789
27	73	;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:
28	72	<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;
29	71	=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<
30	70	>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=
31	69	?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>
32	69	@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?
33	67	ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@
34	66	BCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@A
35	65	CDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@AB
36	64	DEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABC
37	63	EFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCD
38	62	FGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDE
39	61	GHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEF
40	60	HIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFG
41	59	IJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGH
42	58	JKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHI
43	57	KLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJ
44	56	LMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJK
45	55	MNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKL
46	54	NOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLM
47	53	OPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN
48	52	PQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNO
49	51	QRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOP

```
50 50 RSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQ
51 49 STUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQR
52 48 TUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRS
53 47 UVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRST
54 46 VWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTU
55 45 WXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUV
56 44 XYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVW
57 43 YZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWX
58 42 Z[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXY
59 41 [\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ
60 40 \]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[
61 39 ]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\
62 38 ^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]
63 37 _`abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^
64 36 `abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
65 35 abcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
66 34 bcdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`a
67 33 cdefghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ab
68 32 defghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
69 31 efghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcd
70 30 fghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcde
71 29 ghijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdef
72 28 hijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
73 27 ijklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
74 26 jklmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
75 25 klmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
76 24 lmnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
77 23 mnopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
78 22 nopqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
79 21 opqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
80 20 pqrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
81 19 qrstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
82 18 rstuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
83 17 stuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
84 16 tuvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
85 15 uvwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
86 14 vwxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
87 13 wxyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuv
88 12 xyz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvw
89 11 yz{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwx
90 10 z{|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxy
91 09 {|}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz
92 08 |}~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{
93 07 }~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|
94 06 ~áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}
95 05 áéíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
96 04 éíóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~á
97 03 íóú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áé
98 02 óú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéí
99 01 ú !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíó
```

(You may want to trim this part with scissors, so the arrows below are closer to the edge.)

← !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~áéíóú →

space

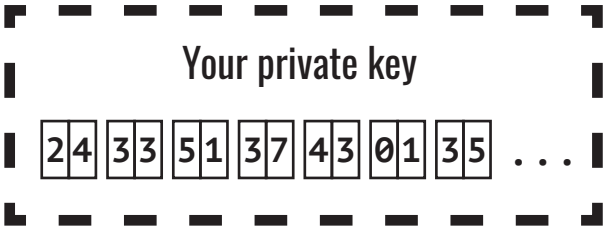
Cursor strip

How does a one-time pad cipher work?

A one-time pad cipher is similar to a rotation cipher, except each character in the plaintext is encoded using its own random rotation value. That way, the ciphertext will look completely random to anyone who doesn't have the private key.

Step 1: Generate a private key

To generate your **private key**, also known as a **pad**, you'll roll your 10-sided die repeatedly to generate random numbers from 00 to 99. Each number in your private key will require two die rolls: one for the first digit, and one for the second digit.



Inside the front cover of this zine, you'll find a grid titled "Your private key" and one titled "A private key for your friend." Roll the die, then write down the digit in both private key grids. Repeat until your private key is as long as you need.

The length of your private key determines the length of the message you'll be able to send. If you use 80 two-digit numbers for your private key, you'll be able to send a plaintext message with up to 80 characters (including spaces and punctuation).

If you want, you can roll two dice to generate random numbers twice as fast. Try to use dice that look different, so you can consistently use one die for the first digit and one for the second digit.

We're choosing random numbers from 00 to 99. That means the cipher needs an "alphabet" of 100 unique characters. The list of characters we'll use (which you can see in the left margin) includes capital letters, lowercase letters, numbers, punctuation marks, and the space character. The first 95 characters, in order, are copied from from the ASCII character set. The last 5 characters are vowels with acute accents.

If you want, you can use the following Python code to print the character set:

```
print(list([chr(i) for i in range(32,127)]) +
["á","é","í","ó","ú"])
```

Why am I rolling a die? Can't computers generate random numbers?

Ordinary computers can't generate random numbers. Instead, they use special algorithms to generate **pseudorandom** numbers, which look like they're chosen at random.

However ... if your adversary is familiar with the pseudorandom number generator you're using, they might be able to deduce the pattern, reconstruct the exact series of pseudorandom numbers you used, and decode your message.

Unlike using a computer, rolling dice can generate truly random numbers.

Step 2: Share the private key with your friend

You should now have two identical copies of your private key. Keep your copy in a safe place, and share the other one with the friend you want to send a message to.

You shouldn't send your private key over any channel that might be under surveillance, because anyone with the private key will be able to read your encrypted message when you send it.

Step 3: Encode your message

Let's encode the words "Meet me" using the example private key. First, find the grid labeled "Plaintext" and write out your message one character at a time. Each character in your message, including spaces and punctuation marks, should go in its own square.

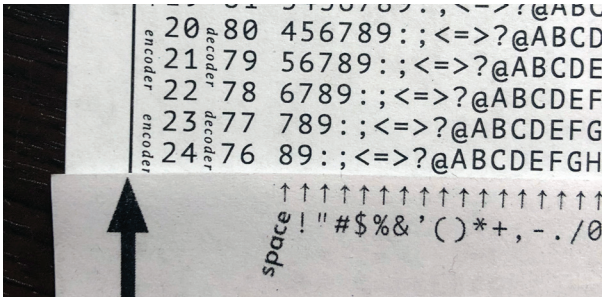
Here's the example plaintext we'll encode:

Plaintext

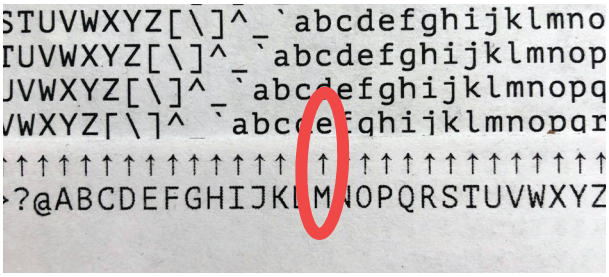
M	e	e	t		m	e	. . .

Each character in your plaintext message corresponds to a two-digit number in your private key. In the example above, the first letter, **M**, corresponds to the number **24** in the provided key.

Turn to the encoder-decoder lookup table and find the **encoder** column on the far left. Align your **cursor strip** with the line labeled **24**, using the arrows as a guide.



Find the letter **M** on the cursor strip and use the arrow above to find the letter you'll use in your ciphertext. In this case, it's the lowercase letter **e**.



Write the letter **e** in your ciphertext grid, then move to the next letter. Here's the complete ciphertext for "Meet me", using the private key from the previous page:

Ciphertext

e	"	4	5	K	n	$	. . .

Step 4: Send your encoded message

Since your message is securely encrypted, you can share it any way you want. Send it by email, chat, mail, or phone. Write it on a wall with spraypaint if you want. As long as you and your friend burn the key and plaintext when you're done (and there aren't any digital copies), no one will ever be able to decode the message.

Use your head. If you send your encrypted message by email, chat, mail, or phone, there's still a lot of metadata being collected. If you and your friend are carrying cell phones when you meet in a remote place, your GPS coordinates will tell the tale.

Also, If you're being actively surveilled, sending encrypted messages could raise a red flag. If that's a concern, you might want to look into steganography (e.g., embedding the ciphertext in an image file).

Step 5: Decode a message

Your friend will decode the message one character at a time, using the **decoder** column in the lookup table.

When decoding, you may find it useful to check off each letter as you go.

Never reuse a private key!

If you reuse a private key, even once, you'll open yourself to frequency analysis attacks.

To avoid mistakes, you should burn everything when you're done. You can easily burn slips of paper in a glass or mug.

Create a pad of numbered keys

If you plan to exchange a series of messages, you can create identical pads of private keys for you and your friend. Then use the keys in order, burning each when you're done.

If someone steals you or your friend's private keys, they can potentially send messages impersonating you. If you want to confirm the sender, you can create a series of passcodes to include with your messages.

Iffy Books

319 N. 11th St. #3D
Philadelphia, PA 19107

Join our email list
at iffybooks.net

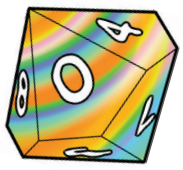
Follow @iffybooks
on social media

Send corrections to
iffybooks@protonmail.com

Published December 2021
at Iffy Books

Version 0.9

Download this zine as a PDF:
https://iffybooks.net/otp



Here's a message for you to decode!

Private key (a.k.a. one-time pad)

39	95	70	30	83	88	04	71
81	25	18	26	34	62	02	27
16	35	45	42	03	85	78	87

Ciphertext

p	á	F	1	T	space	p	g
V	#	2	j	-	M	u	space
r	(	5	:	w	j	n	space